JOURNAL OF NUMBER THEORY 30, 267–287 (1988)

Calibre d'un corps global

R. PAYSANT-LE ROUX

Université de Caen, UFR Sciences, Département de Mathématiques, Esplanade de la Paix, 14032 Caen Cedex, France

Communicated by M. Waldschmidt

Received March 27, 1987; revised January 6, 1988

On se propose de généraliser la notion de calibre d'un corps de nombres quadratique, introduite par Lachaud [prépublication de l'Université de Nice, n° 63, 1984], à un corps de nombres quelconque. Pour cela les notions de points extrémaux dans un module et de module réduits sont utilisées, voir [*J. Number Theory* **15** (1982), 283–294; *J. Number Theory* **26** (1987); "L'arithmétique des corps quadratiques," Monographies de l'enseignement mathématiques, Institut de Mathématiques Université, Genève, 1962; *Acta Arith.* **48** (1987), 9–47; Courbes elliptiques," Séminaire d'algorithmique de Caen, Année 1986–1987; Invariants arithmétiques des corps possédant une formule du produit. Applications," pp. 291–300, SMF Astérisque 147.148, 1987]. Finalement, grâce à un théorème de Siegel ["Algebraic Number Theory," Addison–Wesley, Reading, MA, 1970], on montre qu'il n'existe qu'un nombre fini de corps de nombres de calibre et de degré donnés. © 1988 Academic Press, Inc.

1. INTRODUCTION

La notion de calibre d'un corps quadratique réel a été introduite par G. Lachaud [10]. Dans ce travail, il définit d'abord le calibre d'une classe d'idéaux, qui est la longueur de la période du développement en fraction continue de w_2/w_1 où (w_1, w_2) est une $\mathbb{Z}$-base d'un idéal quelconque de la classe. Cette longueur ne dépend pas du choix de la $\mathbb{Z}$-base de l'idéal choisi. Le calibre du corps quadratique est par définition la somme des calibres des différentes classes. G. Lachaud montre qu'il n'y a qu'un nombre fini de corps quadratiques réels de calibre donné.

Ce sont ces notions que nous généralisons aux corps de nombres et aux corps de fonctions algébriques dont le corps de constantes est fini. Nous étendrons également le résultat de G. Lachaud aux corps de nombres: il n'y a qu'un nombre fini de corps de nombres de degré et de calibre donnés. Pour cela, nous utilisons les concepts de point extrémal dans un module et de module réduit [2, 3, 6, 7], un résultat de Siegel [11] et une inégalité qui généralise l'inégalité suivante, bien connue dans le cas d'un corps quadrati-

0022-314X/88 $3.00

que réel: le produit du régulateur par le nombre de classes est inférieur au calibre du corps, à une constante multiplicative près. Notre inégalité complète l'inégalité de J. Buchmann [3] à savoir: $Cm \leqslant h \cdot R$, où m est le calibre, h le nombre de classe, R le régulateur du corps de nombres, C une constante dépendant du nombre de valeurs absolues réelles et complexes et du nombre de racines de l'unité du corps de nombres.

Dans le cas d'un corps de fonctions algébriques de corps de constantes infini, on peut aussi définir le calibre du corps, mais en général, celui-ci est infini. Par exemple, si le corps de fonctions est $\mathbb{Q}(X, Y)$, avec

$$Y^2 = X^3 + aX^2 + bX + c \qquad (a, b, c \in \mathbb{Q}),$$

on montre (Y. Hellegouarch [8]) que le calibre du corps est le nombre de points rationnels sur la cubique (supposée de genre 1).

2. Notations

On désigne par:

Z l'anneau $\mathbb{Z}$ (resp. $k[X]$), où k est un corps et X une indéterminée.

Q le corps des fractions de Z.

K une extension algébrique de degré n de Q dans laquelle k est algébriquement fermé.

S un ensemble d'indices représentant l'ensemble des valeurs absolues archimédiennes normalisées de K si $Q = \mathbb{Q}$, (resp. qui prolongent la valeur absolue sur $Q = k(X)$ définie par $|X| = \gamma > 1$ ($\gamma = q$ si $k = \mathbb{F}_q$).

s le cardinal de S.

r (resp. $2t$) le nombre de plongements réels (resp. complexes) si $Q = \mathbb{Q}$.

$\mathcal{O}_K$ la fermeture intégrale de Z dans K.

D_K la valeur absolute du discriminant de K, si K est un corps de nombres.

Soient $\omega_1, ..., \omega_n$ une base de $\mathcal{O}_K$ et soient $\mathcal{M}$ un module complet entier de K; on définit la norme de $\mathcal{M}$ par:

$$N(\mathcal{M}) = \det_{\omega_1, ..., \omega_1}(\mu_1, ..., \mu_n)$$

où $\mu_1, ..., \mu_n$ est une base de $\mathcal{M}$. Lorsque K est un corps global on a:

$$|N(\mathcal{M})| = [\mathcal{O}_K : \mathcal{M}].$$

3. Groupe opérant sur un graphe, graphe quotient

Soit un graphe simple $\Gamma = (X, Y)$, non nécessairement fini, où Y est une partie de X^2 (voir [13]); on dira qu'un group G opère sur Γ si:

(i) G opère sur X par $(g, x) \to g(x)$.

(ii) Pour tout $g \in G$, et pout tout $(x, y) \in Y$, on a: $(g(x), g(y)) \in Y$.

Soit $\bar{X}$ l'ensemble quotient X/G, alors on peut définir une partie $\bar{Y}$ de X^2 par la relation:

$$(\bar{x}, \bar{y}) \in \bar{Y} \Leftrightarrow \exists x \in \bar{x}, \exists y \in \bar{y} \qquad \text{tels que } (x, y) \in Y.$$

Il est clair que $(\bar{X}, \bar{Y})$ est un graphe simple et que ce graphe est connexe si (X, Y) est connexe.

DÉFINITION 1. On dira que $\bar{\Gamma} := (\bar{X}, \bar{Y})$ est le graphe quotient de Γ par G.

4. Points extrémaux

DÉFINITION 2. Un sous-ensemble $\mathcal{M}$ de K est appelé un *module complet* de K si

(i) $\mathcal{M}$ est un Z-module;

(ii) $\mathcal{M}$ est de rang maximum.

Remarque 1. Le vocabulaire utilisé ici est celui de "la théorie des nombres" de Borevitch et Chafarevitch.

Comme par la suite nous ne nous intéresserons qu'aux modules complets, le mot module sous-entendra que le module est complet sauf mention expresse du contraire.

DÉFINITION 3. Soit $x \in \mathcal{M} - \{0\}$; on dit que x est un point extrémal de $\mathcal{M}$ si pour tout $y \in \mathcal{M} - \{0\}$ vérifiant $|y|_i \leqslant |x|_i$ pout tout $i \in S$, on a les égalités $|y|_i = |x|_i$ pour tout $i \in S$.

Il revient au même de dire que la classe de x est extrémale pour la relation d'ordre partiel définie dans $\mathcal{M}/R$ par $Cl(u) \leqslant Cl(v)$ si $|u|_i \leqslant |v|_i$ pour tout $i \in S$, où R est la relation d'équivalence définie dans $\mathcal{M}$, par $(u, v) \in R$ si $|u|_i = |v|_i$ pout tout $i \in S$.

Nous désignerons par $\mathcal{E}(\mathcal{M})$ l'ensemble des points extrémaux de $\mathcal{M}$ et, lorsque nous ne considérons qu'un seul module, nous écrirons simplement $\mathcal{E}$ pout désigner cet ensemble.

5. Graphes de classes

DÉFINITION 4. Soient $x, y \in \mathcal{E}$; on dit que x et y sont voisins dans $\mathcal{M}$ si le seul élément z de $\mathcal{M}$ tel que $|z|_i < \mathrm{Sup}(|x|_i, |y|_i)$ pour tout $i \in S$ est l'élément $z = 0$.

On désignera par Y l'ensemble couples de points voisins de $\mathscr{E}$.
Le couple $(\mathscr{E}, Y)$ est un graphe simple.

PROPOSITION 1. *Soient $\mathscr{M}$ et $\mathscr{M}'$ deux modules équivalents (i.e., il existe $\gamma \in K - \{0\}$ tel que $\mathscr{M}' = \gamma\mathscr{M}$). Alors les graphes de points extrémaux de $\mathscr{M}$ et de $\mathscr{M}'$ sont isomorphes.*

Preuve. En effet si x et y sont des points extrémaux de $\mathscr{M}$ il est clair que γx et γy sont des points extrémaux de $\mathscr{M}'$. De plus, si $(x, y) \in Y(\mathscr{M})$ on a:

$$(\gamma x, \gamma y) \in Y(\mathscr{M}'). \quad \blacksquare$$

PROPOSITION 2. *Soit $\mathscr{O}^*(\mathscr{M})$ le groupe des unités de l'anneau des stabilisateurs de $\mathscr{M}$. Alors le group $\mathscr{O}^*(\mathscr{M})$ opère sur $(\mathscr{E}, Y)$.*

Preuve. (1) Soient $x \in \mathscr{E}$ et $u \in \mathscr{O}^*(\mathscr{M})$; il faut montrer que $ux \in \mathscr{E}$. Soit $y \in \mathscr{M} - \{0\}$ tel que $|y|_i \leqslant |ux|_i$, pout tout $i \in S$, on en déduit $|u^{-1}y|_i \leqslant |x|_i$, pour tout $i \in S$ et donc, puisque $x \in \mathscr{E}$ et $u^{-1}y \in \mathscr{M} - \{0\}$; $|u^{-1}y|_i = |x|_i$, pour tout $i \in S$.

(2) Il faut aussi montrer que si $x, y \in \mathscr{E}$ et $(x, y) \in Y$ alors $(ux, uy) \in Y$, ce qui n'est pas difficile en utilisant la définition de Y. $\blacksquare$

La proposition 2 permet de définir le graphe quotient $(\bar{\mathscr{E}}, \bar{Y})$, de $(\mathscr{E}, Y)$ par $\mathscr{O}^*(\mathscr{M})$. Rappelons que $\bar{\mathscr{E}} = (\mathscr{E}/\mathscr{O}^*(\mathscr{M}))$ et que:

$$(\bar{x}, \bar{y}) \in \bar{Y} \Leftrightarrow \exists x \in \bar{x}, \exists y \in \bar{y} \qquad \text{tels que } (x, y) \in Y.$$

Le graphe $(\bar{\mathscr{E}}, \bar{Y})$ sera appelé le graphe des classes de points extrémaux du module $\mathscr{M}$. Il est clair que si deux modules sont équivalents, leurs graphes de classes de points extrémaux sont isomorphes. Ce graphe est donc attaché à la classe du module.

EXEMPLE. Dans le cas d'un corps quadratique réel, le graphe des classes de points extrémaux d'un module $\mathscr{M} = \mathbb{Z}w_1 + \mathbb{Z}w_2$ est un cycle. La longueur du cycle est égale à la longueur de la période du développement en fraction continue de w_2/w_1.

6. MAJORATION DE LA NORME D'UN POINT EXTRÉMAL

DÉFINITION 5. Pour tout $i \in S$, on se donne $c_i \in \mathbb{R}^+ \cup \{\infty\}$ et on écrit $c = (c_1, ..., c_s)$. On pose:

$$\Pi_c = \{x \in K^*, |x|_i < c_i\}, \qquad \text{avec} \quad c = (c_1, ..., c_s).$$

On dit que Π_c est le parallélotope associé à c. Le volume du parrallélotope Π_c sera, par définition, le nombre $c_1 \cdots c_s$ et on écrira:

$$v(\Pi_c) = c_1 \cdots c_s.$$

LEMME 2 (de Minkowski). *Soit $\mathcal{M}$ un module. Il existe une constante $M(\mathcal{M})$ telle que $v(\Pi_c) > M(\mathcal{M})$ entraîne $\Pi_c \cap \mathcal{M} \neq \{0\}$ quelque soit $c \in (\mathbb{R}^+)^s$.*

Si K est un corps de nombres, on peut prendre:

$$M(\mathcal{M}) = \left(\frac{2}{\Pi}\right)^t D_{\mathcal{M}}^{1/2}.$$

$D_{\mathcal{M}}$ désigne la valeur absolule du discriminant du module $\mathcal{M}$.

Si K est un corps de fonction de genre g et si $e = \sum_{i \in S} \deg P_i$, on peut prendre:

$$M(\mathcal{M}) = \gamma^{g+e} |N(\mathcal{M})|^n.$$

Preuve. (1) Lorsque K est un corps de nombres algébriques, c'est le lemme de Minkowski proprement dit.

(2) Lorsque K est un corps de fonctions, on considère le parallélotope "généralisé" faisant intervenir non seulement les valeurs absolues de S mais aussi celles qui divisent $N(\mathcal{M})$:

$$\Pi_c^* = \{x \in K^*, |x|_i < c_i, \forall i \in S \text{ et } |x|_P \leqslant |N(\mathcal{M})|_P, \forall P \in T\}$$

où $T = \{P$ classe de places de K, telles que $P | N((\mathcal{M})\}$.

Désignons par $[x]$ la partie entière de $x \in \mathbb{R}$, posons $e_i = [-\operatorname{Log} c_i / \deg P_i \operatorname{Log} \gamma]$ pout tout $i \in S$, où P_i désigne la place associée à la valeur absolue d'indice i, et définissons un diviseur D_c^* par la relation:

$$D_c^* = \sum_{i \in S} e_i P_i + \sum_{P \in T} v_P(N(\mathcal{M})) \cdot P.$$

D'après le théorème de Riemann, [5, p. 29] on a:

$$l\left(D_c^* + \sum_{i \in S} P_i\right) + \deg\left(D_c^* + \sum_{i \in S} P_i\right) \geqslant 1 - g$$

or:

$$l\left(D_c^* + \sum_{i \in S} P_i\right) \geqslant 1 \Rightarrow \Pi_c^* \cap N(\mathcal{M})\mathcal{O}_K \neq \{0\}$$

et comme $N(\mathcal{M})\mathcal{O}_K \subset \mathcal{M}$, on aura $\Pi_c^* \cap \mathcal{M} \neq \{0\}$.

Il suffit donc de chercher la condition sur c pour que:

$$1-g-\deg\left(D_c^*+\sum_{i\in S}P_i\right)\geqslant 1$$

on trouve comme dans [7]: $v(\Pi_c)\geqslant \gamma^{g+c}|N(\mathcal{M})|^n$. ∎

Remarque 2. Dans le cas d'un corps de fonctions, la constante M trouvée ci-dessus peut être améliorée si on suppose que le module $\mathcal{M}$ est un idéal $\mathcal{A}$ de $\mathcal{O}_K$.

On considère le parallélotope:

$$\Pi_c^*=\{x\in K^*,\ |x|_i<c_i,\ \forall i\in S \text{ et } |x|_P\leqslant|\mathcal{A}|_P,\ \forall P\in T\}$$

où T désigne l'ensemble $\{P,\ P|\mathcal{A}\}$.

En suivant la démontration précédente, on trouve:

$$M(\mathcal{A})=\gamma^{g+c}|N(\mathcal{A})|.$$

PROPOSITION 3. *Soit $\mathcal{M}$ un module et x un point extrémal de $\mathcal{M}$. Si K est un corps de nombres, on a*:

$$|N_{K/Q}(x)|\leqslant\left(\frac{2}{\pi}\right)^t D_{\mathcal{M}}^{1/2}.$$

Si K est un corps de fonctions de genre g et si $h=\min\{\deg P_i,\ i\in S\}$, on a

$$|N_{K/Q}(x)|\leqslant\gamma^{g+h-1}|N(\mathcal{M})|^n.$$

Preuve. (1) Si $Q=\mathbb{Q}$, l'inegalité résulte immédiatement du lemme de Minkowski.

(2) Si $Q=k(X)$ et si on applique le lemme 2, on voit que:

$$|N_{K/Q}(x)|\leqslant\gamma^{g+c}|N(\mathcal{M})|^n.$$

Mais en utilisant le fait que x est un point extrémal, nous pouvons améliorer l'inégalité ci-dessus. Considérons le diviseur:

$$D_x=\sum_{i\in S}P_i^{v_i(x)}+\sum_{P\in T}P^{v_P(N(\mathcal{M}))}:=D_S+D_T,$$

où T est l'ensemble des idéaux premiers de $\mathcal{O}_K$ qui divisent $N(\mathcal{M})$. Le sous-espace vectoriel associé à D_x est l'ensemble des $y\in K$ tels que:

$$\begin{aligned}
&|y|_i\leqslant|x|_i, && \forall i\in S\\
&|y|_P\leqslant|N(\mathcal{M})|_P, && \forall P\in T\\
&|y|_P\leqslant 1, && \forall P\notin S\cup T.
\end{aligned}$$

Comme x est un point extrémal et que $N(\mathcal{M}))\cdot \mathcal{O}_K \subset \mathcal{M}$, on a l'inégalité:

$$l(D_x) := \dim_K L(D_x) \leqslant h.$$

D'autre part, le théorème de Riemann [5, p. 29] nous donne:

$$l(D_x) + \deg D_x \geqslant 1 - g,$$

d'où:

$$\deg_K(D_S) \geqslant -g - h + 1 - \deg_K(D_T),$$

ou encore

$$\deg_K((x) - D_S) \leqslant g + h - 1 + \deg_K(D_T);$$

l'inégalité cherchée suit alors des égalités:

$$\deg_Q(N_{K/Q}((x) - D_S)) = \deg_K((x) - D_S),$$
$$\deg_Q(N_{K/Q}(D_T)) = \deg_K(D_T). \quad \blacksquare$$

Remarque 3. Si $\mathcal{A}$ désigne est un idéal du corps de fonctions K et si $x \in \mathcal{O}_{\mathcal{A}}$, on a:

$$|N_{K/Q}(x)| \leqslant \gamma^{g+h-1} |N(\mathcal{A})|.$$

7. Théorème de Lagrange

Le résultat suivant est particulier aux corps de nombres.

Lemme 3. *Soient α, $\beta \in K$, où K désigne un corps de nombres. Si l'on a $|\alpha|_i \leqslant |\beta|_i$ pour tout $i \in S$ alors on a:*

ou bien $|\alpha|_i = |\beta|_i$ pour tout $i \in S$

ou bien $|\alpha|_i < |\beta|_i$ pour tout $i \in S$.

Preuve. Le cas où $\alpha = 0$ étant trivial, nous poserons $\lambda = \alpha/\beta$ et nous supposerons que $\lambda \in K^*$ est tel que $|\lambda|_i \leqslant 1$, pour tout $i \in S$. Supposons qu'il existe $j \in S$ tel que $|\lambda|_j = 1$. On peut supposer $j = 1$ et on désignera $|x|_1$ par $|x|$ pour tout $x \in K$. Dans le cas où $|\ |$ est réelle, $|\lambda| = 1 \Rightarrow \lambda = \pm 1$ et donc $|\lambda|_i = 1$, pout tout $i \in S$. Dans le cas contraire, supposons que $|\ |$ soit complexe, il vient:

$$|\lambda|^2 = \lambda\bar{\lambda} = 1 \Rightarrow N(\lambda)\, N(\bar{\lambda}) = 1.$$

Or:

$$(N(\lambda))^2 = N(\lambda)\, N(\bar{\lambda}) = 1 \Rightarrow |N(\lambda)| = 1$$

mais $|N(\lambda)| = |\lambda|_1 \cdots |\lambda|_r |\lambda|_{r+1} \cdots |\lambda|_{r+t} = 1$ donc $|\lambda|_i = 1$, pour tout $i \in S$, d'après l'hypothèse $|\lambda|_i \leqslant 1$, pour tout $i \in S$. ∎

LEMME 4. *Soit* $c \in \mathbb{R}_+^s$. *Si* $\Pi_c \cap \mathcal{M} \neq \{0\}$ *alors* $\Pi_c \cap \mathcal{E}(\mathcal{M}) \neq \{0\}$.

Preuve. On peut supposer $\mathcal{M}$ entier et $s \geqslant 2$. Soit $\alpha_1 = \inf\{|y|_1 ; y \in \Pi_c \cap \mathcal{M},\ y \neq 0\}$. Cette borne inférieure est atteinte parce que dans le cas d'un corps de nombres $\Pi_c \cap \mathcal{M}$ est fini, et dans le cas d'un corps de fonctions, on a les inégalités:

$$|y|_1 \geqslant \frac{1}{\prod_{i=2}^{s} |y|_i} \geqslant \frac{1}{c_2 \cdots c_s}$$

et la valeur $|\ |_1$ est discrète. Soit $y \in \Pi_c \cap \mathcal{M}$ tel que $|y|_1 = \alpha_1$. Si K est un corps de nombres le lemme 3 montre que y est un point extrémal. Si K est un corps de fonctions, l'existence d'un élément extrémal dans $\Pi_c \cap \mathcal{M}$ est plus compliquée à prouver puisque le lemme 3 ne s'applique pas. On considère:

$$\Omega_1 = \{ y \in \Pi_c \cap \mathcal{M}, |y|_1 = \alpha_1 \}$$

et on définit par récurrence des ensembles Ω_i et des nombres α_i pour $2 \leqslant i \leqslant s$, par:

$$\alpha_i = \inf\{|y|_i,\ y \in \Omega_{i-1}\}$$
$$\Omega_i = \{ y \in \Omega_{i-1},\ |y|_i = \alpha_i \};$$

finalement on choisit $y \in \Omega_s$. Montrons que y est un point extrémal. En effet si $z \in \mathcal{M} - \{0\}$ et si $|z|_i \leqslant |y|_i$, pour tout $i \in S$ on voit que $z \in \Pi_c \cap \mathcal{M}$ et successivement, que z est dans tous les Ω_j $(1 \leqslant j \leqslant s)$; donc, pour tout $i \in S$, on a $|z|_i = |y|_i$. ∎

Le lemme suivant est démontré dans [7, p. 19].

LEMME 5. *Si K est un corps de nombres ou si le corps des constantes est fini, il n'existe qu'un nombre fini de* $x \in \mathcal{M}$, *non associés, tels que* $N_{K/Q}(x)$ *soit donné.*

THÉORÈME 1 (Théorème de Lagrange). *Soit un module* $\mathcal{M}$ *de K.*

(i) *Le graphe des points extrémaux est connexe.*

(ii) *Lorsque K est un corps global (corps de nombres ou corps de*

fonctions sur un corps de constantes k fini) *le graphe des* classes *de points extrémaux de* $\mathcal{M}$ *est fini et connexe.*

Preuve. (i) Le fait que $\mathscr{E}$ soit fini résulte de la proposition 3 et du lemme 5.

(ii) Pour montrer que le graphe $(\bar{\mathscr{E}}, \bar{Y})$ est connexe, nous allons montrer que $(\mathscr{E}, Y)$ est connexe. On peut supposer $\mathcal{M}$ entier d'après la proposition 1. Soient $x_1, x_2 \in \mathscr{E}$, posons:

$$S(x_1, x_2) = \{ y \in \mathcal{M}, \forall i \in S, |y|_i < \max\{|x_1|_i, |x_2|_i\}\}.$$

— Dans le cas d'un corps de nombres, $S(x_1, x_2)$ est un ensemble fini car $\mathcal{M}$ est entier. Si $S(x_1, x_2) = \{0\}$ alors $(x_1, x_2) \in Y$. Sinon $S(x_1, x_2) \neq \{0\}$ et, d'après le lemme 4, $S(x_1, x_2) \cap \mathscr{E} \neq \{0\}$. Soit $y \in S(x_1, x_2) \cap \mathscr{E}$ et $y \neq 0$ alors $S(x_1, y) \subsetneq S(x_1, x_2)$ et

$$S(y, x_2) \subsetneq S(x_1, x_2).$$

Ainsi en raisonnant par récurrence sur le nombre d'éléments de $S(x_1, x_2)$, on montre que x_1 et x_2 peuvent être peuvent être joints par un chemin.

— Dans le cas d'un corps de fonctions $S(x_1, x_2)$ est un espace vectoriel de dimension finie d'après le théorème de Riemann et Roch, et on suit la même démonstration que précédemment, à ceci près que la récurrence porte sur la dimension de l'espace vectoriel $S(x_1, x_2)$. ∎

Remarque 4. Dans le cas d'un corps quadratique réel (voir [4, 12]) le graphe des points extrémaux est non seulement connexe mais forme une double chaîne infinie (voir remarque 5). Supposons que $\mathcal{M} = \mathbb{Z}w_1 + \mathbb{Z}w_2$ et posons $w = w_2/w_1$, alors cette chaîne est définie par la partie périodique du développement en fraction continue de w. Lorsque l'on passe au graphe quotient, on obtient un cycle dont la longueur est celle de la période. La même remarque vaut pour un corps de fonctions quadratique "réel" sur un corps de constante k fini, c'est-à-dire pour $K = k(X, Y)$, $Y^2 = X^{2p} + a_1 X^{2p-1} + \cdots a_{2p} \in k[X]$ comme l'a montré E. Artin dans [1].

8. Définition d'un i-voisin principal d'un point extrémal

On suppose ici que $s \geqslant 2$.

Définition 6. Soient $i \in S$, $\mathcal{M}$ un module complet et $x \in \mathscr{E}(\mathcal{M})$. Un point $y \in \mathcal{M} - 0$ sera appelé un i-voisin principal de x si:

(1) $y \in \mathscr{E}(\mathcal{M})$,

(2) y est voisin de x,

(3) Pour tout $j \in S$, $j \neq i$, on a:

$$|y|_j < |x|_j.$$

LEMME 6. *Soit $\mathcal{M}$ un module complet et $x \in \mathcal{E}(\mathcal{M})$. Pour tout $i \in S$, x possède un i-voisin principal.*

Preuve. Nous allons reprendre la démonstration du lemme 4, pour simplifier les notations, nous supposerons que $S = \{1, ..., s\}$ et que $i = 1$.

Nous poserons $c = (\infty, |x|_2, ..., |x|_s)$ et

$$\alpha_1 = \inf\{|z|_1 ; \quad z \in \Pi_c \cap \mathcal{M}, z \neq 0\}.$$

(a) Lorsque K est un corps de nombres, cette borne inférieure α_1 existe, et est atteinte, d'après le lemme de Minkowski. Le lemme 3 montre que tout $y \in \Pi_c \cap \mathcal{M}$ tel que $|y|_1 = \alpha_1$ vérifie les conditions de la définition 6.

(b) Lorsque K est un corps de fonctions, le lemme 3 n'est plus valable et la construction ci-dessus ne permet pas de dire que $y \in \mathcal{E}(\mathcal{M})$. Mais la construction du lemme 4 nous donne un élément y de $\mathcal{M}$, non nul, tel que $|y|_1 = \alpha_1$ et tel que $(|y|_2, ..., |y|_s)$ soit minimal pour l'ordre lexicographique. On a montré dans la démonstration du lemme 4 que $y \in \mathcal{E}(\mathcal{M})$. Il ne reste plus qu'à montrer que x et y sont voisins. Soit $z \in \mathcal{M}$ tel que pout tout $i \in S$:

$$|z|_i < \mathrm{Sup}\{|x|_i, |y|_i\}$$

alors on voit que $z \in \Pi_c \cap \mathcal{M}$ en prenant $i \neq 1$ et puisque $|z|_1 < |y|_1 = \alpha_1$, on voit que $z = 0$. ∎

Remarque 5. Lorsque l'on s'est donné un ordre sur S, on constate que tous les i-voisins de x qui sont minimaux pour l'ordre lexicographique sur $S - \{i\}$ sont équivalents pour la relation R (de la définition 3). Mais si K est totalement réel (resp. si toutes les valeurs absolues de S sont de degré un) alors les i-voisin principaux sont uniques au signe près (resp. aux constantes non nules près).

Définition d'une i-chaîne de points extrémaux d'origine x

Soit x un point extrémal d'un module $\mathcal{M}$, la chaîne de points extrémaux:

$$x_0 := x, x_1, ..., x_{n-1}, x_n, ...$$

où x_n est un i-voisin principal de x_{n-1}, $n \geqslant 1$ est appelée une i-chaîne de points extrémaux d'origine x (ou une chaîne de points extrémaux dans la direction i d'origine x) i désignant toujours l'indice d'une valeur absolue de S.

Remarque 6. Si $|S| = 2$ et si R désigne la relation d'équivalence définie après la définition 3 alors $\mathscr{E}/R$ est formé de la réunion des deux i-chaînes dont l'origine est un point extrémal quelconque.

Le lemme suivant montre que la connaissance des voisins principaux d'un point extrémal sert à la détermination de tous les voisins de ce point.

LEMME 7. *Soit ρ un point extrémal de $\mathscr{M}$.*

Si ρ_i, $1 \leqslant i \leqslant s$, sont des i-voisins principaux de ρ alors tout point extrémal ρ' voisin de ρ vérifie:

$$|\rho'|_i \leqslant |\rho_i|_i \qquad \textit{pour tout } i,\ 1 \leqslant i \leqslant s.$$

Preuve. On raisonne par l'absurde; supposons qu'il existe i, $1 \leqslant i \leqslant s$, tel que:

$$|\rho'|_i > |\rho_i|_i.$$

Par définition de ρ_i, $|\rho_i|_j < |\rho|_j$, pour tout $j \neq i$, on a donc les inégalités:

$$|\rho_i|_i < \max(|\rho|_i, |\rho'|_i)$$
$$|\rho_i|_j < \max(|\rho|_j, |\rho'|_j), \qquad \forall j \neq i$$

ce qui contredit l'hypothèse que ρ et ρ' sont voisins. ∎

9. GRAPHE DE MODULES RÉDUITS: CALIBRE D'UN MODULE

Rappelons que le mot module" signifie "module complet" pour nous, c'est-à-dire "Z-module de rang maximal dans K."

DÉFINITION 7. Soit un module $\mathscr{M}$ (ici non nécessairement entier).

L'ensemble des $z \in Q$ tels que $z\mathscr{M} \subset \mathcal{O}_K$ est un Z-module I, qu'on appelle le module des dénominateurs de $\mathscr{M}$.

On notera par $\alpha(\mathscr{M})$ la base normalisée (i.e., positive, resp. fraction rationnelle unitaire) de I. On l'appellera le plus petit dénominateur rationnel de $\mathscr{M}$.

Soit $Cl_1(\mathscr{M})$ l'ensemble des modules $\mathscr{M}'$ équivalents à $\mathscr{M}$ et tels que 1 soit un point extrémal de $\mathscr{M}'$.

PROPOSITION 4. *Soit $\mathscr{M}$ un module et soit $\bar{\mathscr{E}}_{\mathscr{M}}$ l'ensemble des classes de points extrémaux de $\mathscr{M}$ modulo $\mathcal{O}^*(\mathscr{M})$. L'application*

$$\bar{\mathscr{E}}(\mathscr{M}) \to Cl_1(\mathscr{M})$$
$$\rho \mapsto \rho^{-1}\mathscr{M}$$

est une bijection.

Preuve. (1) L'application est bien définie sur $\mathscr{E}(\mathscr{M})$ car si $\varepsilon \in \mathscr{O}^*(\mathscr{M})$ on a:

$$(\varepsilon\rho)^{-1}\mathscr{M} = \rho^{-1}\mathscr{M}.$$

(2) Montrons que l'application est injective. Soient ρ et ρ' deux points extrémaux de $\mathscr{M}$. Supposons que:

$$\rho^{-1}\mathscr{M} = \rho'^{-1}\mathscr{M}$$

il est clair que $\rho/\rho' \in \mathscr{O}^*(\mathscr{M})$.

(3) Montrons que l'application est surjective. Soit $\mathscr{M}' \in Cl_1(\mathscr{M})$ alors il existe $\gamma \in K - \{0\}$ tel que $\mathscr{M}' = \gamma\mathscr{M}$. Si on pose $\rho = 1/\gamma$, 1 étant un point extrémal de $\mathscr{M}'$, ρ est un point extrémal de $\mathscr{M}$ et on a $\mathscr{M}' = \rho^{-1}\mathscr{M}$. ∎

Comme les modules qui sont dans $Cl_1(\mathscr{M})$ ne sont pas entiers, on considère l'ensemble $Cl_e(\mathscr{M})$ défini par:

$$Cl_e(\mathscr{M}) = \{\alpha(\mathscr{M}')\mathscr{M}',\ \mathscr{M}' \in Cl_1(\mathscr{M})\}.$$

PROPOSITION 5. *L'application*

$$Cl_1(\mathscr{M}) \to Cl_e(\mathscr{M})$$
$$\mathscr{M} \mapsto \alpha(\mathscr{M})\mathscr{M}$$

est une bijection.

Si de plus $\mathscr{M}' \in Cl_e(\mathscr{M})$, $\mathscr{M}'$ *est primitif* (*i.e.*, $\alpha(\mathscr{M}') = 1$).

Preuve.

• Montrons que l'application est injective. Soient $\mathscr{M}'$, $\mathscr{M}'' \in Cl_1(\mathscr{M})$ tels que

$$\alpha(\mathscr{M}')\mathscr{M}' = \alpha(\mathscr{M}'')\mathscr{M}'' := \mathscr{N},$$

$\alpha(\mathscr{M}') \in Q$ et est un point extrémal de $\mathscr{N}$ (et $\alpha(\mathscr{M}')$ est normalisé"), $\alpha(\mathscr{M}'') \in Q$ et est un point extrémal de $\mathscr{N}$ (et $\alpha(\mathscr{M})$ est normalisé"). On en déduit l'égalité: $\alpha(\mathscr{M}') = \alpha(\mathscr{M}'')$ et donc $\mathscr{M}' = \mathscr{M}''$.

• Si $\mathscr{N} \in Cl_e(\mathscr{M})$ alors $\mathscr{N}$ est-il primitif? Ceci résultera du lemme suivant. ∎

LEMME 8. *Soit* $\mathscr{M}$ *un module de* K

(1) *Si* $\gamma \in Q - \{0\}$ *et si* γ *est normalisé on a:* $\alpha(\gamma\mathscr{M}) = \gamma^{-1}\alpha(\mathscr{M})$.

(2) *Si* $1 \in \mathscr{M}$ *alors* $\alpha(\mathscr{M})$ *est entier et le module* $\alpha(\mathscr{M})\mathscr{M}$ *est entier et primitif.*

Preuve. (1) Résulte de la définition 7.

(2) Montrons que le plus petit dénominateur du module $\mathscr{M}$ est entier.

En effet $\alpha(\mathscr{M}) \in \mathcal{O}_K$ car $1 \in \mathscr{M}$, mais $\alpha(\mathscr{M}) \in Q$ par définition, donc:

$$\alpha(\mathscr{M}) \in \mathcal{O}_K \cap Q = Z.$$

Enfin le module $\alpha(\mathscr{M})\mathscr{M}$ est entier par définition de $\alpha(\mathscr{M})$ et primitif d'après le (1). ∎

Notation. Si ρ est un point extrémal de $\mathscr{M}$ alors $\alpha(\rho^{-1}\mathscr{M})$ est le point extrémal entier (i.e., appartenant à Z) du module $\alpha(\rho^{-1}\mathscr{M})\rho^{-1}\mathscr{M}$. On désignera ce dernier module par $\mathscr{M}_\rho$:

$$\mathscr{M}_\rho := \alpha(\rho^{-1}\mathscr{M})\rho^{-1}\mathscr{M}.$$

DÉFINITION 8. Soit $\mathscr{M}$ un module de K.

L'ensemble $J = Z \cap \mathscr{M}$ est un Z-module. On notera par $\beta(\mathscr{M})$ une base normalisée de J et on l'appellera le plus petit entier rationnel de $\mathscr{M}$.

Remarque 7. D'après le lemme 8 et le fait que $\alpha(\rho^{-1}\mathscr{M})$ est le point extrémal entier (i.e., appartenant à Z) du module $\alpha(\rho^{-1}\mathscr{M})\rho^{-1}\mathscr{M}$. On désignera ce dernier module par $\mathscr{M}_\rho$:

DÉFINITION 9. Un module $\mathscr{M}$ de K est dit réduit si

(1) $\mathscr{M}$ est entier.

(2) $\mathscr{M}$ est primitif (i.e., $\alpha(\mathscr{M}) = 1$).

(3) $\beta(\mathscr{M})$ est un point extrémal de $\mathscr{M}$.

Notons par $\mathscr{R}_{\mathscr{M}}$ l'ensemble des modules réduits équivalents à $\mathscr{M}$.

THÉORÈME 2. *L'application*

$$\begin{aligned} \bar{\mathscr{E}}(\mathscr{M}) &\to \mathscr{R}_{\mathscr{M}} \\ \rho &\mapsto \alpha(\rho^{-1}\mathscr{M})\rho^{-1}\mathscr{M} := \mathscr{M}_\rho \end{aligned}$$

est une bijection.

DÉFINITION 10. $\mathscr{M}_\rho$ est appelé le *module réduit associé à* ρ *et à* $\mathscr{M}$, on a donc $\mathscr{M}_\rho := \alpha(\rho^{-1}\mathscr{M})\rho^{-1}\mathscr{M}$.

Remarque 8. Le théorème 2 permet de parler du graphe des modules réduits d'un module $\mathscr{M}$.

Preuve. Elle résulte des deux propositions précédentes et de l'égalité

$$Cl_e(\mathcal{M}) = \mathcal{R}_{\mathcal{M}}.$$

En effet, $Cl_e(\mathcal{M}) \subset \mathcal{R}_{\mathcal{M}}$ résulte du lemme 8 et de la remarque 7. Montrons que $\mathcal{R}_{\mathcal{M}} \subset Cl_e(\mathcal{M})$. Soit $\mathcal{M}' \in \mathcal{R}_{\mathcal{M}}$, $\mathcal{M}' = \gamma\mathcal{M}$, $\gamma \in K - \{0\}$. Posons $\rho = \gamma^{-1}\beta(\mathcal{M}')$, on a alors $\mathcal{M}' = \beta(\mathcal{M}')\rho^{-1}\mathcal{M}$ et il reste à montrer que $\beta(\mathcal{M}') = \alpha(\rho^{-1}\mathcal{M})$. On $\alpha(\rho^{-1}\mathcal{M})$ divise $\beta(\mathcal{M}')$ car $\mathcal{M}'$ est entier, donc il existe $d \in Z$ tel que:

$$\beta(\mathcal{M}') = d\alpha(\rho^{-1}\mathcal{M})$$

et donc:

$$\mathcal{M}' = d\mathcal{M}_\rho$$

$\mathcal{M}_\rho$, $\mathcal{M}'$ étant tous les deux primitifs, l'égalité précédente implique que $d \in Z^*$, par suite

$$\beta(\mathcal{M}') = \alpha(\rho^{-1}\mathcal{M}). \quad \blacksquare$$

PROPOSITION 6. *Deux modules équivalents ont les mêmes modules réduits. D'une manière précise, si $\mathcal{M}$ et $\mathcal{M}'$ sont équivalents on a $\mathcal{R}_{\mathcal{M}} = \mathcal{R}_{\mathcal{M}'}$.*

Preuve. Soient $\mathcal{M}$ et $\mathcal{M}'$ deux modules équivalents

$$\mathcal{M} = \gamma\mathcal{M}', \quad \gamma \in K - \{0\}.$$

On veut montrer que pout tout $\rho \in \mathcal{E}(\mathcal{M})$, il existe $\rho' \in \mathcal{E}(\mathcal{M}')$ tel que $\mathcal{M}_\rho = \mathcal{M}'_{\rho'}$, or

$$\mathcal{M}_\rho = \alpha\rho^{-1}\mathcal{M}, \qquad \text{où} \quad \alpha = \alpha(\rho^{-1}\mathcal{M})$$

on a donc les égalités:

$$\alpha\rho^{-1}\mathcal{M} = \alpha\rho^{-1}\gamma\mathcal{M}' = \alpha\rho'^{-1}\mathcal{M}'$$

si on pose $\rho' = \rho\gamma^{-1}$, qui est un point extrémal de $\mathcal{M}'$. Par hypothèse, $\alpha\rho^{-1}\mathcal{M}$ est inclus dans $\mathcal{O}_K$ et donc par définition de $\alpha(\rho^{-1}\mathcal{M}')$ on déduit que $\alpha(\rho'^{-1}\mathcal{M}') \mid \alpha$.

Par symétrie, on a aussi $\alpha \mid \alpha'$ et donc $\alpha = \alpha' := \alpha(\rho^{-1}\mathcal{M}')$. $\blacksquare$

Remarque 9. La proposition 6 permet de voir que le graphe de modules réduits est attaché à la classe de $\mathcal{M}$ et non à $\mathcal{M}$.

DÉFINITION 11. Le nombre de modules réduits équivalents à un module $\mathcal{M}$ est appelé le calibre du module $\mathcal{M}$ ou le calibre de la classe de $\mathcal{M}$.

10. Calibre d'un corps global

THÉORÈME 3. *Soit K un corps global (i.e., un corps de nombres ou un corps de fonctions algébriques dont le corps des constantes est fini).*

Soient $\mathscr{J}$ l'ensemble des idéaux fractionnaires de K, $\mathscr{P}$ l'ensemble des idéaux principaux de K; alors le nombre d'éléments de $\mathscr{J}/\mathscr{P}$ est égal au nombre de composantes connexes du graphe fini des idéaux réduits.

Preuve. Le graphe des idéaux réduits associés à un idéal $\mathscr{A}$ étant connexe (théorème 1) on définit l'application:

$$\mathscr{J} \to \mathscr{C} = \text{ensemble des composantes connexes du graphe des idéaux réduits de } K.$$

$$\mathscr{A} \to \text{graphe des idéaux réduits de } \mathscr{A}.$$

Deux éléments de $\mathscr{J}$ donnent la même image si et seulement si ils sont équivalents (proposition 6), on en déduit que l'application considérée passe au quotient et définit une injection de $\mathscr{J}/\mathscr{P}$ dans $\mathscr{C}$. ∎

Nous sommes maintenant en mesure de généraliser la notion de calibre d'un corps global (voir Lachaud [10]).

DÉFINITION 12. Posons $\mathscr{H}(K) = \mathscr{J}/\mathscr{P}$.
On appelle calibre du corps global K le nombre

$$m(K) = \sum_{\mathscr{C} \in \mathscr{H}(K)} m(\mathscr{C})$$

où $m(\mathscr{C})$ est le calibre d'un idéal $\mathscr{A}$ de la classe $\mathscr{C}$.

Remarque 10. Tout corps de calibre 1 est principal.

LEMME 9. *Soit $\mathscr{M}$ un module, on a l'inégalité*

$$|N(\mathscr{M})| \leqslant |\beta(\mathscr{M})^n| \, |N(\mathscr{O}(\mathscr{M}))|.$$

Preuve. (1) Supposons $\mathscr{M} \subset \mathscr{O}(\mathscr{M})$ et utilisons le théorème de structure sur les modules de type fini sur un anneau principal.

Il existe une Z-base $e_1, ..., e_n$ de $\mathscr{O}(\mathscr{M})$ et un n-uple $(a_1, ..., a_n) \in Z^n$ tels que $\mathscr{M} = Za_1e_1 \oplus \cdots \oplus Za_ne_n$, $a_1 | a_2 |, ..., | a_n$, où a_n est normalisé (i.e., positif, resp. polynôme unitaire).

(1.1) Montrons que $a_n = \beta(\mathscr{M})$.

(1.1.1) a_n divise $\beta(\mathscr{M})$.

Montrons que pour tout $a \in \mathcal{M} \cap Z$, $a_n \mid a$ donc que a_n divise $\beta(\mathcal{M})$. En effet $ae_n \in \mathcal{M}$ car $e_n \in \mathcal{O}(\mathcal{M})$ d'où $ae_n = da_n e_n$, avec $d \in Z$.

(1.1.2) $\beta(\mathcal{M})$ divise a_n.

Pour cela montrons que $a_n \in \mathcal{M} \cap Z$, en effet:

$$a_n = a_n 1 = a_n \left(\sum_{i=1}^{n} x_i e_i \right), \qquad x_i \in Z$$

donc:

$$a_n = \sum_{i=1}^{n} y_i (a_i e_i) \in \mathcal{M}, \qquad \text{car } a_i \mid a_n, \text{ pour tout } i,\ 1 \leqslant i \leqslant n.$$

(1.2) Finalement, on obtient

$$|N_{\mathcal{O}(\mathcal{M})}(\mathcal{M})| = |a_1 \cdots a_n| \leqslant |a_n|^n = |\beta(\mathcal{M})|^n.$$

(2) Le résultat, pour un module quelconque, résulte de l'existence d'un $d \in Z$, avec d normalisé tel que:

$$d\mathcal{M} \subset \mathcal{O}(\mathcal{M})$$

et de l'égalité $\beta(d\mathcal{M}) = d\beta(\mathcal{M})$. ∎

LEMME 10. *Soit $\mathcal{M}$ un module primitif, on a l'inégalité*

$$|N(\mathcal{M})| \leqslant |\beta(\mathcal{M})|^{n-1} |N(\mathcal{O}(\mathcal{M}))|.$$

Preuve. Il existe une Z-base $(e_1, ..., e_n)$ de $\mathcal{O}(\mathcal{M})$, un n-uple $(a_1, ..., a_n) \in Z^n$ et un entier $d \in Z$, normalisé tels que:

$$d\mathcal{M} = Za_1 e_1 \oplus \cdots \oplus Za_n e_n, \qquad a_1 \mid a_2 \mid \cdots \mid a_n, \ a_1 \text{ et } a_n \text{ normalisés.}$$

On peut supposer que $(d, a_1) = 1$. On a donc:

$$\mathcal{M} = \frac{a_1}{d} \left(Z_{e_1} \oplus \cdots \oplus Z \frac{a_n}{a_1} e_n \right).$$

Montrons que $a_1 = 1$. Pour cela nous raisonnerons par l'absurbe en supposant que $a_1 \neq 1$. Soit p un nombre premier qui divise a_1. Puisque $\mathcal{M}$ est primitif, il existe $x \in \mathcal{M}$ tel que p ne divise pas x, mais

$$dx = a_1 \left(\lambda_1 e_1 + \cdots + \lambda_n \frac{a_n}{a_1} e_n \right), \qquad \text{avec} \quad \lambda_i \in Z$$

donc p divise dx, comme p ne divise pas d, p divise x, ce qui est contradictoire. On a donc:

$$|N_{\mathcal{O}(\mathcal{M})}(\mathcal{M})| = \left|\frac{a_2 \cdots a_n}{d^n}\right| \leqslant \left|\frac{a_n}{d}\right|^{n-1}$$

or on a montré dans la preuve du lemme 9, que

$$\beta(d\mathcal{M}) = a_n$$

or $\beta(d\mathcal{M}) = d\beta(\mathcal{M})$ donc:

$$|N_{\mathcal{O}(\mathcal{M})}(\mathcal{M})| \leqslant |\beta(\mathcal{M})|^{n-1}. \quad \blacksquare$$

Remarque 11. Si $\mathcal{A}$ est un idéal réduit et si $n=2$, l'inégalité du lemme 10 est l'égalité bien connue:

$$|N(\mathcal{A})| = |\beta(\mathcal{A})|.$$

LEMME 11. *Soit $\mathcal{A}$ un idéal réduit. Si K est un corps de nombres, on a:*

$$|\beta(\mathcal{A})| \leqslant (2/\pi)^t D_K^{1/2} \tag{1}$$

$$|N(\mathcal{A})| \leqslant (2/\pi)^{t(n-1)} D_K^{(n-1)/2}. \tag{2}$$

Si K est un corps de fonctions de genre g et si $h = \min\{\deg P_i,\ i \in S\}$, on a:

$$|\beta(\mathcal{A})| \leqslant \gamma^{g+h-1} \tag{1'}$$

$$|N(\mathcal{A})| \leqslant \gamma^{(g+h-1)(n-1)}. \tag{2'}$$

Preuve. $\beta(\mathcal{A})$ étant un point extrémal de $\mathcal{A}$, on a d'après la proposition 3:

$$|\beta(\mathcal{A})|^n = |N_{K/Q}(\beta(\mathcal{A}))| \leqslant (2/\pi)^t N(\mathcal{A}) D_K^{1/2}, \quad \text{si } K \text{ est un corps de nombres.} \tag{3}$$

$$|N(\mathcal{A})|^n = |N_{K/Q}(\beta(\mathcal{A}))| \leqslant \gamma^{g+h-1} |N(\mathcal{A})|, \quad \text{si } K \text{ est un corps de fonctions.} \tag{3'}$$

$\mathcal{A}$ étant primitif, le lemme 10 nous donne l'inégalité:

$$|N(\mathcal{A})| \leqslant |\beta(\mathcal{A})|^{n-1}. \tag{4}$$

On déduit l'inégalité (1) de (3) et (4) et l'inégalité (1') de (3') et (4). En revenant à l'inégalité (4), on obtient (2) et (2'). $\blacksquare$

LEMME 12. *On suppose $s \geqslant 2$. Soient ρ et ρ' deux points extrémaux voisins dans un idéal de K. Si K est un corps de nombres, on a*

$$|\rho'/\rho|_i \leqslant (2/\pi)^r D_K^{1/2} \qquad \text{pour} \quad 1 \leqslant i \leqslant s. \tag{5}$$

Si K est un corps de fonctions de genre g et si $e = \sum_{i \in S} \deg P_i$ on a:

$$|\rho'/\rho|_i \leqslant \gamma^{g+e} \qquad \text{pour} \quad 1 \leqslant i \leqslant s. \tag{5'}$$

Preuve. (1) Soit $\mathcal{A}_\rho$ l'idéal réduit associé au point extrémal ρ; on a:

$$\mathcal{A}_\rho = \alpha(\rho)\, \rho^{-1} \mathcal{A}$$

en posant $\alpha(\rho) := \alpha(\rho^{-1}\mathcal{A})$. On sait (proposition 1) que ξ est un point extrémal de $\mathcal{A}_\rho$ voisin de $\alpha(\rho)$ si et seulement si

$$\rho' = \rho\alpha(\rho)^{-1}\xi \text{ est un point extrémal de } \mathcal{A} \text{ voisin de } \rho. \tag{6}$$

De plus, si ξ_i est un i-voisin principal de $\alpha(\rho)$ dans $\mathcal{A}_\rho$ alors $\rho_i' = \rho\alpha(\rho)^{-1}\xi_i$ est un i-voisin principal de ρ. C'est cette dernière propriété, jointe au lemme de Minkowski qui va nous permettre de montrer les inégalités (5) et (5').

(2) Si ξ_i est un i-voisin principal de $\alpha(\rho)$ dans $\mathcal{A}_\rho$ nous montrerons plus loin que l'on a:

$$|\xi_i|_i \leqslant N \frac{|\alpha(\rho)|_i}{|\alpha(\rho)|} \tag{7}$$

où N vaut $(2/\pi)^r D_K^{1/2}$ si K est un corps de nombres, resp. γ^{g+e} si K est un corps de fonctions.

Le lemme 7 entraîne alors que:

$$|\xi|_i \leqslant N \frac{|\alpha(\rho)|_i}{|\alpha(\rho)|} \tag{8}$$

pour tout point extrémal ξ voisin de $\alpha(\rho)$ dans $\mathcal{A}_\rho$.

(3) Faisons la démonstration de l'inégalité (7) pour $i = 1$. D'après le lemme 2 (de Minkowski), il existe $\xi \in \mathcal{A}_\rho \setminus \{0\}$ tel que

$$|\xi|_j < |\alpha(\rho)|_j \quad \text{si} \quad j \neq 1, \qquad \text{et} \qquad |\xi|_1 < M \frac{|\alpha(\rho)|_1}{|\alpha(\rho)|^n}. \tag{9}$$

L'expression de M donnée dans le lemme 2 et la remarque 2 puis les relations:

$$\alpha(\rho) = \beta(\mathcal{A}_\rho), \qquad D_{\mathcal{A}} = |N_{\mathcal{C}_K}(\mathcal{A}_\rho)|\, D_K^{1/2}, \qquad |N_{\mathcal{C}_K}(\mathcal{A}_\rho)| \leqslant |\alpha(\rho)|^{n-1}$$

entraînent finalement:

$$|\xi|_j < |\alpha(\rho)|_j \text{ si } j \neq 1 \qquad \text{et} \qquad |\xi|_1 < N\frac{|\alpha(\rho)|_1}{|\alpha(\rho)|} \tag{10}$$

avec N égal à:

$$\begin{cases} (2/\pi)^r D_K^{1/2} & \text{si } K \text{ est un corps de nombres} \\ \gamma^{g+e}, & \text{si } K \text{ est un corps de fonctions.} \end{cases} \tag{11}$$

D'après la définition d'un 1-voisin principal de $\alpha(\rho)$ dans $\mathscr{A}_\rho$, on voit que ξ_1 vérifie (7) pour $i=1$.

(4) De l'égalité (6), de l'inégalité (8) et de $|\alpha(\rho)| \geqslant 1$, on déduit que, pour tout i, tel que $1 \leqslant i \leqslant s$:

$$\left|\frac{\rho'}{\rho}\right|_i = \left|\frac{\xi}{\alpha(\rho)}\right|_i \leqslant N. \quad \blacksquare$$

THÉORÈME 4. *On suppose que $s \geqslant 2$. Soit K un corps de nombres; on a l'inégalité*:

$$hR \leqslant C[m(K)]^{s-1}$$

où R est le régulateur du corps, h est le nombre de classes d'idéaux (i.e., $\#\mathscr{H}(K)$), $C=(s-1)^{(s-1)/2}(\mathrm{Log}((2/\pi)^r D_K^{1/2}))^{s-1}$ ($2t$ désigne le nombre de plongements complexes de K).

Preuve. Soient $\mathscr{A}$ un idéal de K, i un élément de S et ε_i une unité de $\mathscr{O}_K$ construite à l'aide d'une i-chaîne de ponts extrémaux du module $\mathscr{A}$. On sait [6] que $(s-1)$ quelconque de ces s unités sont indépendantes, d'où l'inégalité:

$$R \leqslant v \cdot a \begin{vmatrix} \mathrm{Log}\,|\varepsilon_1|_1, \ldots, \mathrm{Log}\,|\varepsilon_{s-1}|_1 \\ \cdots \\ \mathrm{Log}\,|\varepsilon_1|_{s-1}, \ldots, \mathrm{Log}\,|\varepsilon_{s-1}|_{s-1} \end{vmatrix}$$

d'où, d'après l'inégalité de Hadamard on a:

$$R \leqslant \left(\prod_{i=1}^{s-1}\left(\sum_{j=1}^{s-1} \log |\varepsilon_i{}^j|\right)^2\right)^{1/2}$$

or, par construction, l'unité ε_i est de la forme:

$$\varepsilon_i = \frac{\rho^{(i)}_{n_1^{(i)}}}{\rho^{(i)}_{n_2^{(i)}}} = \frac{\rho^{(i)}_{n_1^{(i)}}}{\rho^{(i)}_{n_1^{(i)}-1}} \cdot \frac{\rho^{(i)}_{n_1^{(i)}-1}}{\rho^{(i)}_{n_1^{(i)}-2}} \cdots \frac{\rho^{(i)}_{n_2^{(i)}+1}}{\rho^{(i)}_{n_2^{(i)}}}, \qquad \text{avec } n_1^{(i)} > n_2^{(i)} \tag{12}$$

où les $\rho_k^{(i)}$, $n_2^{(i)} \leqslant k \leqslant n_1^{(i)}$, sont les points extrémaux successifs (non équivalent deux à deux) appartenant à une i-ème chaîne de $\mathscr{A}$.

De l'égalité (12) on déduit:

$$|\varepsilon_i|_i \leqslant \left(\operatorname{Sup}_k \left| \frac{\rho_{k+1}^{(i)}}{\rho_k^{(i)}} \right|_i \right)^{n_1^{(i)} - n_2^{(i)}}$$

or on a, d'une part, l'inégalité:

$$n_1^{(i)} - n_2^{(i)} \leqslant m(\mathscr{C}) \qquad \text{ou} \quad \mathscr{C} = Cl(\mathscr{A})$$

et, d'autre part (lemme 12):

$$\left| \frac{\rho_{k+1}^{(i)}}{\rho_k^{(i)}} \right|_i \leqslant \left(\frac{2}{\pi} \right)^t D_K^{1/2}.$$

Posons:

$$E = \left(\frac{2}{\pi} \right)^t D_K^{1/2}.$$

On a donc l'inégalité:

$$|\varepsilon_i|_i \leqslant E^{m(\mathscr{C})}.$$

On en déduit aussi:

$$|\varepsilon_i|_j \geqslant E^{-m(\mathscr{C})} \qquad \text{si} \quad j \neq i.$$

car par construction des ε_i, $|\varepsilon_i|_j < 1$ si $j \neq i$ et:

$$\prod_{j=1}^{s} |\varepsilon_i|_j = |N(\varepsilon_i)| = 1.$$

Finalement, on obtient les inégalités:

$$|\operatorname{Log} |\varepsilon_i|_j| \leqslant m(\mathscr{C}) \operatorname{Log}(E) \qquad \text{pour} \quad 1 \leqslant j \leqslant s$$

et donc

$$R \leqslant (s-1)^{(s-1)/2} [m(\mathscr{C})]^{s-1}.$$

En sommant sur $\mathscr{H}(K) = \mathscr{J}/\mathscr{P}$ et en utilisant l'inégalité

$$\sum_{\mathscr{C} \in \mathscr{H}(K)} [m(\mathscr{C})]^{s-1} \leqslant [m(K)]^{s-1}$$

on obtient le résultat. ∎

THÉORÈME 5. *Soit un entier n fixé. Il n'y a qu'un nombre fini de corps de nombres de degré n ayant un calibre donné.*

Preuve. Si $s = 1$, le résultat est classique. Supposons donc $s \geqslant 2$. D'après un résultat de Siegel (voir Lang [11]), on sait que $\operatorname{Log} hR \sim \operatorname{Log} D_k^{1/2}$ quand D_K tend vers l'infini, K étant un corps de nombres de degré n. Joint à l'inégalité du théorème précédent, ceci montre que si $m(K)$ est fixé, D_K est majoré. ∎

Remarque 12. Ce dernier résultat n'est pas effectif dans la mesure où le théorème de Siegel, utilisé ici, ne l'est pas.

RÉFÉRENCES BIBLIOGRAPHIQUES

1. E. ARTIN, Quadratischer Körper im Gebiet der höheren Kongruenzen I, II, *Math. Z.* **19** (1924), 153–246.
2. H. APPELGATE ET ONISHI, Periodic expansion of modules and its relation to units, *J. Number Theory* **15** (1982), 283–294.
3. J. BUCHMANN, (a) On the computation of units and class numbers by generalization of Lagrange's algorithm; (b) On the period length of the generalized Lagrange algorithm, *J. Number Theory* **26** (1987), 8–37.
4. A. CHATELET, "L'arithmétique des corps quadratiques," Monographies de l'enseignement mathématiques, Institut de Mathématiques, Université, Genève, 1962.
5. M. DEURING, "Lectures on the Theory of Algebraic Functions of One Variables, Lecture Notes in Maths, Vol. 314, Springer-Verlag, New York/Berlin, 1973.
6. Y. HELLEGOUARCH ET R. PAYSANT-LE ROUX, "Commas, points extrémaux et arêtes des corps possédant une formule du produit," C.R.M., Ac. Sc. Canada, 1985.
7. Y. HELLEGOUARCH, D. L. MCQUILLAN, ET R. PAYSANT-LE ROUX, Unités de certains sous-anneaux des corps de fonctions algébriques, *Acta Arith.* **48** (1987), 9–47.
8. Y. HELLEGOUARCH, "Courbes elliptiques," séminaire d'algorithmique de Caen, Année 1986–1987.
9. Y. HELLEGOUARCH ET R. PAYSANT-LE ROUX, "Invariants arithmétiques des corps possédant une formule du produit. Applications," pp. 291–300, SMF Astérisque 147.148, 1987.
10. G. LACHAUD, "Calibre et fonctions zéta des corps quadratiques réels," prépublication de l'Université de Nice, n° 63, 1984.
11. S. LANG, "Algebraic Number Theory," Addison-Wesley Reading, MA, 1970.
12. S. LOUBOUTIN, "Arithmétique des corps quadratiques réels et fractions continues," Thèse de Doctorat, Université Paris 7, juin, 1987.
13. R. J. WILSON, "Introduction to Graph Theory," Longmans, Greens, New York, 1979.